(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 March 2005 (17.03.2005)

PCT

(10) International Publication Number
WO 2005/025178 A1

(51) International Patent Classification[7]: H04L 29/06

(21) International Application Number: PCT/IB2004/002815

(22) International Filing Date: 30 August 2004 (30.08.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
03292219.7 9 September 2003 (09.09.2003) EP

(71) Applicant *(for all designated States except US)*: **AXALTO SA** [FR/FR]; Intellectual Property Department, 50 avenue Jean Jaurès, F-92120 Montrouge (FR).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **BERNARD, Eddy** [FR/FR]; c/o Axalto SA, Intellectual Property Department, 50 avenue Jean Jaurès, F-92120 Montrouge (FR). **SALGADO, Stéphanie** [FR/FR]; c/o Axalto SA, Intellectual Property Department, 50 avenue Jean Jaurès, F-92120 Montrouge (FR).

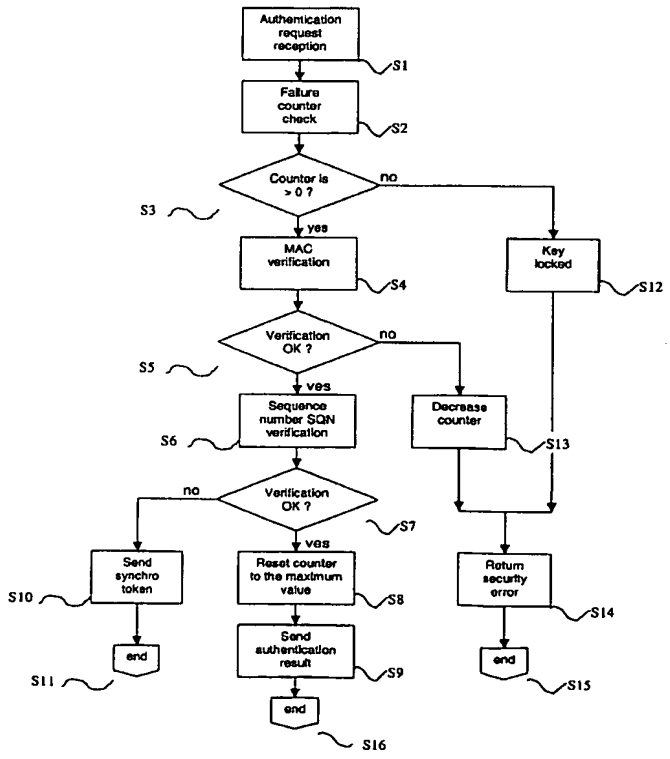
(74) Common Representative: **AXALTO SA**; c/o Vincent YQUEL, Intellectual Property Department, 50 avenue Jean Jaurès, F-92120 Montrouge (FR).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,

[Continued on next page]

(54) Title: AUTHENTICATION METHOD IN DATA COMMUNICATION AND SMART CARD FOR IMPLEMENTING THE SAME



(57) Abstract: The invention sets forth an authentication method for use in a system including a first entity and a second entity in a network, the first entity being adapted to authenticate the second entity and data received therefrom, both first and second entities storing the same secret key. The method is implemented in a smart card such as a USIM card, including : a memory storing authentication algorithms and keys; means for receiving a message authenticating code and other parameters; means for computing an expected code from said other parameters and from said secret key; means for comparing said message authenticating code received and said expected code; and means for aborting authentication if the message authenticating code received and the expected code do not match. The smart card further comprises a failure counter adapted to store the number of abortion occurrences, and means for updating said failure counter every time the comparing means indicate that said message authenticating code and said expected code do not match. Thanks to its built-in failure counter and the fact that the updating of this counter is controlled from inside the card, the card becomes tamper-resistant against reiterated fraudulent authentication attempts.

WO 2005/025178 A1

ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:

— *of inventorship (Rule 4.17(iv)) for US only*

Published:

— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.